UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/519,827 | 12/21/2005 | Michael Jacobs | CHAP-005 | 3097 |

36822 7590 10/27/2009

GORDON & JACOBSON, P.C.
60 LONG RIDGE ROAD
SUITE 407
STAMFORD, CT 06902

| EXAMINER | |
|---|---|
| WRIGHT, BRYAN F | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2431 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 10/27/2009 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/519,827 | JACOBS, MICHAEL | |
| | Examiner | Art Unit | |
| | BRYAN WRIGHT | 2431 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *04 August 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *63-72* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *63-72* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

### *Continued Examination Under 37 CFR 1.114*

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 8/4/2009 has been entered. Claims 43-62 are cancelled. Claims 63-72 has been added. Claims 63-72 are pending.

### *Claim Rejections - 35 USC § 112*

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

1. Claim 63 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The Examiner contends applicant's newly added limitation step (h) for which reads "authenticating said second data file by generating a hash value for said second data file and comparing the hash value for the second data file generated in (h)

with the hash value for said second data file published in said dated journal", lacks support of original disclosure. Specifically, the operation of generating a hash value for said second data file. The Examiner respectfully interprets applicant's claim limitation element of "second data file" to be equivalent to applicant's "MDH", in accordance with applicant's original specification paragraph 7. The Examiner contends paragraph 7 recites that "MDH" is sent over to the third party and is maintained for comparison purpose. No where does applicant recite or imply that a hash of the "MDH" is performed as claimed.

2. Claims 67, 69 and 72 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Applicant's claim limitation of "the receiver transmitting the purported copy of said second hash value to the third party" lacks support of original disclosure.

.

***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claim 71 is rejected under 35 U.S.C. 102(b) as being anticipated by Toh et al. (US Patent Publication No. 2002/0004902 and Toh hereinafter).

4. As to claim 71, Toh teaches a method for verifying by a recipient the authenticity of use of an identifier by a sender, said method comprising:

(i) identifying the communication of a message encrypted using a secret key unique to said sender from said sender to said recipient across an information technology communications network (i.e., ...teaches sender authentication [par. 67]);

(ii) accessing, in response to said identification, storage means (e.g., account profile) containing information relating to the most recent message encrypted using said secret key which has occurred across said information technology communications network (i.e., ... teaches the recipient accessing account profile to connect with the OC for the purpose of receiving the encrypted message [par, 70]);

(iii) obtaining confirmation (e.g., notification ) from said sender that said most recent event is valid (e.g., successful ) [par. 86],

(iv) preventing further use of said secret key in the event that said confirmation is not received (i.e., ...teaches the ability to revoke a key [par. 50 & 65]).

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claim 72 is rejected under 35 U.S.C. 103(a) as being unpatentable over Toh.

6. As to claim 72, Toh teaches a method further comprising: the sender generating a first hash value of said message (i.e., ...teaches the sender generating a hash value of the data to be transmitted [par. 58]);

the sender encrypting said message with a first secret key and producing a second hash value from said encrypted message (i.e., .. teaches performing an encryption operation before sending the message [par. 58]);

the sender encrypting said first secret key with a second secret key (i.e., …teaches the receiver receives an encrypted document decryption key [par. 67]);

the sender transmitting to the receiver said encrypted message, said encrypted first secret key (e.g., encrypted document decryption key) and said first hash value (i.e., .. teaches the sender sending the encrypted data [par. 67] ... the encrypted data comprising a message, a decryption key, and hash value [par. 67]);

the sender transmitting said second hash value and said second secret key to a third party (i.e., ...teaches a third party receives an hash value and encrypted message [par. 58]);

the receiver (e.g., OC) receiving said encrypted message and generating a purported copy of said second hash value of said encrypted message (i.e., ...teaches the receiver receiving the encrypted message, decrypting the message and performing a hash operation [par. 67]);

the third party determining whether the purported copy matches said second hash value (i.e., ..teaches a third party comparison operation between hashes [par. 58]);

and the third party then releasing said second key if a match is so determined (i.e., .. .teaches upon successful verification of hash key information then delivered to the recipient [par. 67]).

Toh does not expressly teach as claimed:

the third party storing the transmitted second hash value and second secret key for audit purposes;

However given Toh's disclosure of a third party performing a hash operation for the purpose of validation comparison, this would imply to those skilled in the art that Toh would have to have previously stored a hash value in order to have a hash value to compare too [par. 58]. Therefore this would also imply that inherent to Toh's hash capability is Toh's ability to store a given hash value at a

third party. The audit element of applicant's claim limitation indirectly is related to Toh disclosing the ability to maintain hash values for the purpose of validation comparison. Also, Toh does teach storing key data (e.g., secret key) [par. 69]. The key data Toh discloses is from both sender and receiver. Therefore given the implied teachings of Toh in this regard, one of ordinary skill in the art would recognize the benefit of storing hash values to enhance the hash comparison process.

Toh does not expressly teach as claimed:

the receiver transmitting the purported copy of said second hash value to the third party,

However Toh does disclose the ability to exchange data between a receiver and third party for verification purposes and the ability for the receiver to perform a hash operation on received data (e.g., second hash value) [par. 39 & 67]. (The Examiner notes that the specification lacks a specific example to clearly interpret this limitation and as such the Examiner has interpreted this limitation under the broadest reasonable interpretation and consistent with what is common in the art). Consistent with what is known in the art, a third party in a message exchange system is commonly used for authentication or privacy. Therefore given Toh's teachings of data exchange between receiver and third party (e.g., OC) and the receiver ability to perform a hash function, it would have been obvious to those skilled in the art to have a receiver possess the ability to send a

copy of a generated hash to a third party to enhance the message (e.g., second hash value) authentication process.

7. Claims 63-66 are rejected under 35 U.S.C. 103(a) as being unpatentable over Toh in view of Haber et al. (US Patent No. 5,781,629 and Haber herenafter).

8. As to claim 63, Toh teaches a method of permitting authentication of data comprising:

(a) storing copies of a plurality of data items (e.g., ... local storage [par. 36]);

(d) transmitting said single hash value to a remote location (e.g., Operation Center) (i.e.,... teaches sending encrypted hash of the data package to Operation Center [par. 58]), via an information technology communications network [fig. 2];

Toh does not teach:

(b) generating a first data file comprising a respective hash value of each said plurality of stored data items;

(c) generating a single hash value of said first data file derived from said hash values of said plurality of stored data items;

(e) creating at said remote location a second data file comprising said single hash value and one or more additional data items relating to said single hash value;

(f) generating a hash value for said second data file;

and (g) publishing said hash value for said second data file in a journal for authenticating said second data file.

(h) authenticating said second data file by generating a hash value for said second data file and comparing the hash value for the second data file generated in (h) with the hash value for said second data file published in said dated journal.

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Toh as introduced by Haber. Haber discloses:

(b) generating a first data file comprising a respective hash value of each said plurality of stored data items (to generate a data structure (e.g., table) comprising hash values of data items [col. 5, lines 52-56]);

(c) generating a single hash value of said first data file derived from said hash values of said plurality of stored data items (to generate a single hash linked to a number of hash values [col. 3, lines 60-67]);;

(e) creating at said remote location (e.g., service bureau) a second data file comprising said single hash value and one or more additional data items relating to said single hash value (to provide the capability to create a second document (e.g., second data file) at a remote location [col. 5, lines 44-48]);

(f) generating a hash value for said second data file (to provide the capability to generate a hash value for the second document [col. 5, lines 45-50]).

(g) publishing said hash value for said second data file in a journal for authenticating said second data file (to provide the capability to publish a hash value [col. 6, lines 45-60]).

(h) authenticating said second data file by generating a hash value for said second data file and comparing the hash value for the second data file generated in (h) with the hash value for said second data file published in said dated journal (to provide authentication capability involving computing a hash a secondary hash of a stored data item [col. 6, lines 65-67; col. 7, lines 1-5]).

Therefore, given Toh's ability to transmit a hash to a remote location, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Toh to enhance hash maintainability by employing the well known feature of publishing hash values as disclosed above by Haber.

9. As to claim 64, Toh teaches a method where said first data file is generated in (b) at the end of a predetermined time period (par. 86).

10. As to claim 65, Toh teaches a method where: said first data file (e.g., delivery) contains at least one identifier selected from the group consisting of a

file name, a path name, a file size and a time stamp (i.e., ... teaches delivery content including header information (e.g., address information) [par. 67]).

11. As to claim 66, Toh teaches a method where least one of said first data items comprises a message to be transmitted from a sender to a receiver [par. 67].

12. Claims 67-70 are rejected under 35 U.S.C. 103(a) as being unpatentable over Toh.

13. As to claims 67 and 69, Toh teaches a method further comprising: the sender generating a first hash value of said message (i.e., ...teaches the sender generating a hash value of the data to be transmitted [par. 58]);

the sender encrypting said message with a first secret key and producing a second hash value from said encrypted message (i.e., .. teaches performing an encryption operation before sending the message [par. 58]);

the sender encrypting said first secret key with a second secret key (i.e., ...teaches the receiver receives an encrypted document decryption key [par. 67]);

the sender transmitting to the receiver said encrypted message, said encrypted first secret key (e.g., encrypted document decryption key) and said first hash value (i.e., .. teaches the sender sending the encrypted data [par. 67] ...

the encrypted data comprising a message, a decryption key, and hash value [par. 67]);

the sender transmitting said second hash value and said second secret key to a third party (i.e., ...teaches a third party receives an hash value and encrypted message [par. 58]);

the receiver (e.g., OC) receiving said encrypted message and generating a purported copy of said second hash value of said encrypted message (i.e., ...teaches the receiver receiving the encrypted message, decrypting the message and performing a hash operation [par. 67]);

the third party determining whether the purported copy matches said second hash value (i.e., ..teaches a third party comparison operation between hashes [par. 58]);

and the third party then releasing said second key if a match is so determined (i.e., .. .teaches upon successful verification of hash key information then delivered to the recipient [par. 67]).

Toh does not expressly teach as claimed:

the third party storing the transmitted second hash value and second secret key for audit purposes;

However given Toh's disclosure of a third party performing a hash operation for the purpose of validation comparison, this would imply to those skilled in the art that Toh would have to have previously stored a hash value in order to have a

hash value to compare too [par. 58]. Therefore this would also imply that inherent to Toh's hash capability is Toh's ability to store a given hash value at a third party. The audit element of applicant's claim limitation indirectly is related to Toh disclosing the ability to maintain hash values for the purpose of validation comparison. Also, Toh does teach storing key data (e.g., secret key) [par. 69]. The key data Toh discloses is from both sender and receiver. Therefore given the implied teachings of Toh in this regard, one of ordinary skill in the art would recognize the benefit of storing hash values to enhance the hash comparison process.

Toh does not expressly teach as claimed:

the receiver transmitting the purported copy of said second hash value to the third party,

However Toh does disclose the ability to exchange data between a receiver and third party for verification purposes and the ability for the receiver to perform a hash operation on received data (e.g., second hash value) [par. 39 & 67]. (The Examiner notes that the specification lacks a specific example to clearly interpret this limitation and as such the Examiner has interpreted this limitation under the broadest reasonable interpretation and consistent with what is common in the art). Consistent with what is known in the art, a third party in a message exchange system is commonly used for authentication or privacy. Therefore given Toh's teachings of data exchange between receiver and third party (e.g.,

OC) and the receiver ability to perform a hash function, it would have been obvious to those skilled in the art to have a receiver possess the ability to send a copy of a generated hash to a third party to enhance the message (e.g., second hash value) authentication process.

14. As to claim 68 and 70, Toh teaches a method where the first secret key is symmetric and the second secret key is asymmetric (i.e., .. teaches the use of both symmetric and asymmetric keys [par. 28 & 29]).

***Response to Arguments***

With regards to applicant remarks of, "New claim 63 is directed to a method of authenticating data including, inter alia, "... (b) generating a first data file comprising a respective hash value of each said plurality of stored data items; (c) generating a single hash value of said first data file derived from said hash values of said plurality of stored data items; (d) transmitting said single hash value to a remote location, via an information technology communications network; (e) creating at said remote location a second data file comprising said single hash value and one or more additional data items relating to said single hash value; (f) generating a hash value for said second data file; (g) publishing said hash value for said second data file in a dated journal of record published in numerous copies and held in separate public libraries; and (h) authenticating said second data file by generating a hash value for said second data file and comparing the hash value for the second data file generated in (h) with the hash

value for said second data file published in said dated journal (emphasis added)." Nowhere does the cited prior art teach or suggest these features", the Examiner respectfully draws applicant's attention to the 103 rejection above of independent claim 63 made under Toh in view of Harber. The Examiner contends that the 103 rejection details all relevant teachings as they pertain to applicant's newly submitted claim 63.

With regards to applicant's remark of, "Toh does not address the use of hash values to authentic a number of data items, let alone the steps of (b) - (h) as recited in claim 63", the Examiner contends applicant explains in newly added claim 66, that at least one of the data items comprises a message sent from a sender to a receiver. Refer to newly added claim 66. The Examiner respectfully submits Toh and Harber teaches the ability to use a hash operation for the purpose of authenticating a message. Refer to Toh paragraph 58 and Harber column. 6, lines 65-67 & column 7, lines 1-5.

With regards to applicant's remarks of, "Haber does not remedy the shortcomings of Toh. More specifically, Haber describes a user transmitting a request 20 to a remote service bureau. The request includes a hash value 21 for a particular document", the Examiner contends the applicant has defined at least one data item is a message sent between sender and receiver. The Examiner respectfully submits there exists an exact relevancy in this regard to the

teachings of Toh paragraph 58, where Toh discloses the use of a hash function to authenticate a message (e.g., data item).

With regards to applicant's remarks of, "Accordingly, claim 63 is clearly patentable over the cited prior art. The dependent claims 64-68 are patentable over the cited prior art for those reasons advanced above with respect to claim 63 from which they respectfully depend and for reciting additional features that are neither taught or suggested by the cited prior art", the Examiner respectfully traverses applicant's position of patentability and respectfully draws applicant's attention to the 103 rejection of claims 64-68 above made under Toh in view of Harber. The Examiner contends that the 103 rejection details all relevant teaching of the prior art as they pertain to applicants newly submitted claims 64-68.

With regards to applicant's remark of, "New claim 69 is directed to a method of enabling proof by a third party both of transmission of a message from a sender to a receiver and receipt of said message by said receiver, which includes: "... the sender generating a first hash value of said message; the sender encrypting said message with a first secret key and producing a second hash value from said encrypted message; the sender encrypting said first secret key with a second secret key; the sender transmitting to the receiver said encrypted message, said encrypted first secret key and said first hash value; the sender transmitting said second hash value and said second secret key to said

third party; the third party storing the transmitted second hash value and second secret key for audit purposes; the receiver receiving said encrypted message and generating a purported copy of said second hash value of said encrypted message; the receiver transmitting the purported copy of said second hash value to the third party; the third party checking that the purported copy matches said second hash value; and the third party then releasing said second key if a match is determined." Nowhere does the cited prior art teach or suggest these features. Accordingly, claim 69 is clearly patentable over the cited prior art", the Examiner respectfully traverses applicant's position of patentability and respectfully draws applicant's attention to the 103 rejection of claim 69 above made under Toh in view of Harber. The Examiner contends that the 103 rejection details all relevant teaching of the prior art as they pertain to applicants newly submitted claim 69.

With regards to applicant remarks of, "Dependent claim 70 is patentable over the cited prior art for those reasons advanced above with respect to claim 69 from which it respectfully depends and for reciting additional features that are neither taught or suggested by the cited prior art", the Examiner respectfully traverses applicant's position of patentability and respectfully draws applicant's attention to the 103 rejection of claim 70 above made under Toh in view of Harber. The Examiner contends that the 103 rejection details all relevant teaching of the prior art as they pertain to applicants newly submitted claim 70.

With regards to applicant's remarks of, "New claim 71 is directed to a method for verifying by a recipient the authenticity of use of an identifier by a sender, which includes: "... (i) identifying the communication of a message encrypted using a secret key unique to said sender from said sender to said recipient across an information technology communications network; (ii) accessing, in response to said identification, storage means containing information relating to the most recent message encrypted using said secret key which has occurred across said information technology communications network; (iii) obtaining confirmation from said sender that said most recent event is valid, and (iv) preventing further use of said secret key in the event that said confirmation is not received." Nowhere does the cited prior art teach or suggest these features. Accordingly, claim 71 is clearly patentable over the cited prior art", the Examiner respectfully traverses applicant's position of patentability and respectfully draws applicant's attention to the 103 rejection of claim 71 above made under Toh in view of Harber. The Examiner contends that the 103 rejection details all relevant teaching of the prior art as they pertain to applicants newly submitted claim 71.

With regards to applicant's remarks of, "Dependent claim 72 is patentable over the cited prior art for those reasons advanced above with respect to claim 71 from which it respectfully depends and for reciting additional features that are neither taught or suggested by the cited prior art", the Examiner respectfully traverses applicant's position of patentability and respectfully draws applicant's

attention to the 103 rejection of claims 71 and 72 above made under Toh in view of Harber. The Examiner contends that the 103 rejection details all relevant teaching of the prior art as they pertain to applicants newly submitted claims 71 and 72.

***Contact Information***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRYAN WRIGHT whose telephone number is (571)270-3826. The examiner can normally be reached on 8:30 am - 5:30 pm Monday -Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on (571) 272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BRYAN WRIGHT/
Examiner, Art Unit 2431

/William R. Korzuch/
Supervisory Patent Examiner, Art Unit 2431